

REMARKS

In the Office Action dated January 13, 2003, the Examiner noted a typographical error in claim 1, which has been corrected.

Additionally, the rejection of claims 1 and 3 under 35 U.S.C. §103(a) as being unpatentable over French in view of Emmett et al was maintained. Claims 4 and 5 were rejected under 35 U.S.C. §103(a) as being unpatentable over French in view of Emmett, further in view of Gerst. Claims 6-9 were rejected under 35 U.S.C. §103(a) as being unpatentable over French in view of Emmett, further in view of SNA Architecture from IBM Corp.

Applicants note with appreciation the interview courteously afforded the undersigned counsel for the Applicants, at which the Examiner's Supervisor, Mr. Thomas Dickson, also was present. The teachings of the French reference, as discussed below were discussed at the interview with regard to their applicability to all pending claims of the application.

As discussed at the interview, it is the position of the Applicants that the French reference operates in a different manner from the Emmett reference, and therefore regardless of whether the Examiner's characterizations of the teachings of those two references is correct, it would not have been obvious to a person of ordinary skill in the art to modify the French reference in accordance with the teachings of Emmett et al.

The subject matter disclosed and claimed in the present application is for protecting security data in a security module, but still allowing, under appropriate conditions, the security module to be removed from a circuit board, which automatically causes an erasure of the security data stored therein, and then re-

initialized. For this purpose, as set forth in claim 1, a first function unit monitors proper insertion of the security module on the device motherboard and signals a security-related status of the security module. If it is detected that the security module is improperly used or improperly replaced, the second function unit causes the security data in the security module to be erased. If the use and replacement are determined to be proper, however, the first function unit re-initializes the security module, i.e. replaces any erased security data, and the security module is re-commissioned for use.

As explained at the interview, it is well known in the field of postal security technology, for preventing tampering with a postal meter, to employ a postal security module or device (PSD) which is encapsulated in a manner making tampering with the PSD very difficult, and which also is mounted on a circuit board in a manner which allows the removal of the PSD from the circuit board to be monitored. If and when the PSD is removed from the circuit board, it is known to automatically erase the security data stored therein (which usually will be unused postal funds which are electronically stored in the PSD). Therefore, if a person tampering with the postage meter attempts to remove a PSD with available postage stored therein, that person will not be able to use the PSD to frank mail items elsewhere, because the postage data (security data) stored therein will automatically be erased.

The present invention proceeds from the recognition that there are some circumstances, such as when the postage meter is being serviced in a service call by a technician, that the PSD may be legitimately removed temporarily from the circuit board. The present invention allows this to occur and then allows the replacement of

the PSD by the technician, with a re-initialization of the erased data, so that the PSD can continue to be used under such circumstances.

In the French reference, a physical key is inserted in a receptacle of a security device, the security device being connected between a power source and another device to be protected, such as a radio. The protected device cannot be used without the key being inserted into the receptacle of the security device. Therefore, if the protected device is stolen, the thief cannot use the stolen device because the thief will (presumably) not have the proper key to insert in the security device.

As discussed at the interview, however, the French reference does not operate by electronically storing security data in a memory or programming a memory with a security code. Instead, the key in the French reference includes a signal generator which generates a pulse width modulated (PWM) signal, having a duty cycle. As explained in the paragraph beginning at column 4, line 42 of the French reference, and as set forth in claims 7, 8 and 9 thereof, the key is "programmed" by employing a particular circuit element (resistor R_1) having a particular value.

When the key is inserted in the receptacle in the French device, as explained in columns 5 and 6 of the French reference, a window comparator determines whether the duty cycle of the PWM signal (i.e. the area under the pulses) is within a window set by an upper limit value and a lower limit value. The upper threshold of the window of the window comparator, as explained in the paragraph beginning at column 7, line 1 of the French patent, is set via a resistive divider comprised of three resistors 144, 146 and 148. The value of the resistor 148 is programmed by two

additional resistors, 150 and 152, using respective switches 154 and 156. The resistor 148, and the resistors 150 and 152, define the lower limit.

Therefore, no data are "stored" in the receptacle device in the French reference, in the manner that the term "storing data" is commonly understood by those of ordinary skill in the art. The particular duty cycle of the key in the French reference is set by circuit elements, and whether the duty cycle of the PWM signal is sufficient to unlatch the blockage of power to the protected device is determined by whether this duty cycle falls within the aforementioned window. This window, in turn, is set by specific values of circuit elements in the receptacle device.

As discussed at the interview, Applicants submit that selecting particular values for physical circuit components in the context of designing or constructing a circuit is not considered by those of ordinary skill in the art as "storing" data in the circuit. If this were true, then every circuit that was ever designed or built would be a "storage" circuit, which is certainly not the understanding of those ordinary skill in the art.

Moreover, the Examiner has relied on the Emmett et al reference as teaching that it is known in the field of postal security technology to automatically erase security data in a security module if and when the security module is removed from a circuit board. This concept of erasing data, however, makes sense and is applicable only if the data are electronically stored. The idea of "erasure" does not even conceptually apply to the French patent, since as noted above the values for "matching" the key to the receptacle are not stored data at all, but are physical values of circuit components. It is not seen how those physical values of circuit

components could be "erased" even if the concept of the Emmett et al reference were attempted to be applied to the French patent.

As discussed at the interview, Applicants acknowledge that in substantiating a rejection based on two or more references under 35 U.S.C. §103, it is not necessary for the Examiner to explain how a device disclosed in one reference can be physically embodied or physically combined with a device disclosed in another reference. Nevertheless, Applicants respectfully submit it is incumbent on the Examiner to propose more than a combination of concepts. Applicants submit it is incumbent on the Examiner to at least propose a combination which has some hope of resulting in a practical, operational device. As noted above, even if a person of ordinary skill in the art had knowledge of the "erasing" concept in Emmett et al, there is no way to apply that concept to the differently operating circuit in the French patent.

At the interview, it was proposed to amend independent claim 1 as set forth above to explicitly state that the security data are stored in a non-volatile memory of the security module. It was agreed at the interview that this would preclude continued reliance on the French patent as a basis for rejecting the claims of the application, but of course the Examiner is free to conduct further searching. Since the Examiner and his Supervisor at the interview stated that making this change in claim 1 at this time would raise a new issue requiring further searching or consideration, claim 1 has been amended by filing an RCE.

Since all of the rejections made by the Examiner in the Final Rejection rely on the French reference as the primary reference, amending claim 1 in the manner

proposed at the interview is responsive to all of those rejections, regardless of the teachings of the secondary references.

Early consideration of the RCE is therefore respectfully requested.

Submitted by,

Steven H. Noll

(Reg. 28,982)

SCHIFF, HARDIN & WAITE

CUSTOMER NO. 26574

Patent Department

6600 Sears Tower

233 South Wacker Drive

Chicago, Illinois 60606

Telephone: 312/258-5790

Attorneys for Applicants.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS

Claim 1 has been amended as follows:

1. (Twice amended) A method for protecting a security module comprising the steps of:

storing security relevant data in a non-volatile memory of a security module
and inserting said security module in a device motherboard;

monitoring proper insertion of said security module on said device
motherboard with a first function unit and a second function unit in said
security module;

signaling at least one security-related status of said security module with said
first function unit;

detecting at least one of improper use and improper replacement of said
security module with said second function unit and, upon a detection of at least one
of said improper use and said improper replacement, said second function unit
causing said security-relevant data to be erased;

following at least one of proper [u se] use and proper replacement of said
security module, re-initializing, with said first function unit, any erased, security-
relevant data; and

after said re-initializing, enabling each of said first function unit and said
second function unit to re-commission said security module.